



Clear Desk Policy

Version: 4.0

Date: 23/09/2024

thesovereigntrust.uk

The Sovereign Trust is a Multi Academy Trust registered in England No. 09666511. Registered Office: Manor Academy Sale, Manor Avenue, Sale M33 5JX




Document Control

Title	Clear Desk Policy
Supersedes	3.0
Owner	CEO
Circulation/Distribution	All
Review Period	Annually

The Sovereign Trust is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with Trust's policy review schedule.

A current version of this document is available to all interested parties [The Sovereign Trust Website](#)

Signature: 

Date: 23/09/2024

Version History

Next Review Date		23/09/2024		
Version	Date	Amendments	Author	Status
1.0	06/05/2018	Initial Issue	CEO	Approved
2.0	19/08/2021	Updated reference to UK GDPR	CEO	Approved
3.0	03/08/2022	Formatting amendments	CEO	Approved
3.0	23.11.2023	P.4 – taking data offsite -Change to department manager P.5 – Compliance – Change to HR manager	CEO	Approved
4.0	23/09/2024	Included a few additional security measures	CEO	Approved

Introduction

The Sovereign Trust ("Trust") aims to implement and maintain data protection measures to ensure that personal data is secured away appropriately to assist in the reduction of risk of unauthorised access, loss and damage to information.

This policy/guidance checklist is designed to give staff assistance on how to secure personal information (both paper and electronic). This policy/guidance applies to all staff, including temporary and agency staff.

Good Practice

Staff must abide by the following practice points when handling personal data.

Leaving a room

Whenever a room is unoccupied for a short period of time, you should do the following:

- Lock your computer(windowsL).
- Ensure there is no personal data on your desk that can be seen.

Whenever a room is unoccupied for an extended period of time, you should do the following:

- Remove all sensitive and confidential paperwork from plain sight and lock it in a drawer or filing cabinet. This includes mass storage devices such as USB drives and hard drives or laptops and iPads.
- Draws should be locked, and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.
- Devices should be screen-locked and locked away.
- Rooms should be locked.

Confidential waste

- All waste paper which contains sensitive or confidential information must be disposed of either by using the school's onsite secure disposal (shredders) or placed in the designated confidential waste bins.
- Under no circumstances should this information be placed in regular waste paper bins.
- If the school destroy large-scale files such as pupil files or HR records, they should be recorded on the data destruction log.

Computer Screens

- Devices such as iPads/laptops/Chromebooks/tablets/USB sticks must be locked away at the end of the day.
- Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- Computer/laptop screens are to be locked when left unattended.
- An appropriate passcode/password must be set for all accounts. Passwords must be complex (a mix of letters, numbers and special characters) and must not be shared with others.
- Office screens may have privacy screens to prevent people from accidentally viewing information that they are not supposed to see.
- Devices are configured to automatically lock after a period of inactivity.

Displays

- Passwords should not be left in open areas which are visible to others.
- Sensitive or confidential personal data displayed in classrooms should not be left visible or displayed to unauthorised persons.
- Personal data (including but not limited to seating plans, allergy details and student lists) shall be stored in folders or in secure places.
- When sharing screens with the class, staff should ensure that no personal data is shared on the projector. If this happens, staff need to report this to Lisa-Marie Flynn and/or Ian Green, as this will be considered a data breach.
- Before displaying any names and photos, the Academy/School will ensure that the student/parent has provided consent.
- The Trust will limit the amount of data on displays. If names are necessary, only first names will be used.

Taking data offsite

- You are responsible for the security of the data in your possession, and when transporting it offsite, you must always take steps to keep it secure.
- Paper documents should not be removed from the Trust without the prior permission of the department manager. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular, the information is not to be transported in see-through bags or other unsecured storage containers.
- Paper documents should not be used in public spaces and should not be left unattended in any place where they are at risk (e.g., in car boots or a luggage rack on public transport).
- Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed.

- Paper documents are collected from printers as soon as they are produced and not left where they can be casually read.
- The master copy of the data is not to be removed from the Trust premises.
- Paper documents containing personal data are locked away in suitable facilities, such as secure filing cabinets in the home, just as they would be in the Trust.
- Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them.
- Paper documents are disposed of securely by shredding and should not be disposed of with ordinary waste unless it has been shredded first.

Printing

- Any print jobs containing personal information should be retrieved immediately.
- To release printing, the school will use PINS personal to the user.

Compliance

If you have misplaced any information, then you must let your line manager know as quickly as possible.

These guidelines will be monitored for compliance by the senior leadership team and may include random or scheduled inspections and walkthroughs.